МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ

https://doi.org/10.26565/1684-8489-2025-2-03
УДК 351:004.056

Дзюндзюк Вячеслав Борисович,
доктор наук з державного управління, професор,
завідувач кафедри публічної політики
навчально-наукового інституту "Інститут державного управління"
Харківського національного університету імені В. Н. Каразіна, майдан Свободи,
4, м. Харків, 61022, Україна

e-mail: 7vbdzun@gmail.com *https://orcid.org/0000-0003-0622-2600*

ЦИФРОВА ТРАНСФОРМАЦІЯ ПУБЛІЧНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Анотація. Стаття присвячена дослідженню цифрової трансформації систем публічного управління національною безпекою в умовах гібридної війни. На основі аналізу сучасних теоретичних підходів та практичного досвіду провідних країн світу розкрито особливості застосування цифрових технологій у протидії гібридним загрозам. Обґрунтовано необхідність переходу від традиційних бюрократичних моделей забезпечення безпеки до інтегрованих цифрових екосистем, здатних оперативно виявляти, аналізувати та нейтралізувати багатовимірні загрози в реальному часі. Розроблено концептуальну модель цифровізації системи національної безпеки, яка охоплює чотири ключові виміри: інституційний (створення координаційних структур та механізмів міжвідомчої взаємодії), технологічний (впровадження штучного інтелекту, великих даних, блокчейну та кібербезпеки), процесний (оптимізація швидкості прийняття рішень та якості реагування), людський (розвиток цифрових компетенцій персоналу). Визначено пріоритетні напрями цифровізації: системи раннього виявлення загроз на основі машинного навчання, кіберзахист критичної інфраструктури, протидія дезінформації через автоматизовану верифікацію контенту, цифрова розвідка та аналітика, захищені комунікаційні платформи для координації. Окрему увагу приділено інституційним механізмам реалізації цифрової трансформації: створення центру координації, міжвідомчі платформи обміну даними, державно-приватне партнерство, міжнародна кооперація. На прикладі України проаналізовано виклики та можливості цифровізації безпекового сектору в умовах активної фази війни, зокрема успішний досвід цифрових ініціатив «Дія», кібервійськ, IT Army. Встановлено, що ефективність цифрової трансформації залежить від синергії технологічних інновацій, інституційних реформ та культурних змін в організаціях сектору безпеки. Запропоновані рекомендації можуть бути використані для удосконалення державної політики у сфері національної безпеки та оборони.

Ключові слова: цифрова трансформація, національна безпека, гібридна війна, публічне управління, кібербезпека, штучний інтелект, протидія дезінформації, цифрові технології.

Як цитувати: Дзюндзюк В. Б. Цифрова трансформація публічного управління національною безпекою в умовах гібридної війни. *Актуальні проблеми державного управління*. 2025. № 2 (67). С. 60–74. https://doi.org/10.26565/1684-8489-2025-2-03

In cites: Dziundziuk, V.B. (2025). Digital transformation of public administration of national security in conditions of hybrid warfare. *Pressing Problems of Public Administration, 2 (67), 60–74.* https://doi.org/10.26565/1684-8489-2025-2-03 [in Ukrainian].

Вступ. Сучасний безпековий ландшафт характеризується радикальною трансформацією природи загроз та методів їх реалізації. Гібридна війна як феномен XXI століття інтегрує воєнні, політичні, економічні, інформаційні та кібернетичні виміри впливу, створюючи багатовимірні виклики для національної безпеки держав. На відміну від традиційних форм збройного протистояння, гібридні загрози характеризуються асиметричністю, прихованістю джерел походження, поєднанням конвенційних та неконвенційних засобів, цілеспрямованою експлуатацією вразливостей демократичних суспільств.

Російська агресія проти України яскраво демонструє еволюцію гібридної війни від концептуальної моделі до практики масштабного застосування. Починаючи з 2014 року, Україна зіткнулася з комплексом взаємопов'язаних загроз: кібератаками на критичну інфраструктуру, масштабними дезінформаційними кампаніями, фінансуванням сепаратистських рухів, дипломатичним тиском, економічними санкціями та, зрештою, повномасштабною збройною агресією у 2022 році. Ця багаторівнева загроза вимагає відповідно складної, інтегрованої та швидкої відповіді з боку систем національної безпеки.

Традиційні бюрократичні моделі публічного управління безпекою, сформовані в епоху індустріального суспільства, демонструють критичні обмеження у протидії гібридним загрозам. Ієрархічні структури, фрагментація відповідальності між відомствами, повільні процедури обміну інформацією, відсутність інтероперабельності інформаційних систем – все це унеможливлює своєчасне виявлення та адекватне реагування на динамічні, мережеві, транскордонні загрози. Розрив між швидкістю розгортання гібридних атак (що вимірюється годинами чи хвилинами в кіберпросторі) та швидкістю бюрократичного реагування (що вимірюється днями чи тижнями) створює стратегічну вразливість демократичних держав.

Цифрова трансформація систем національної безпеки постає не просто як технологічна модернізація, а як фундаментальна зміна парадигми публічного управління безпекою. Впровадження штучного інтелекту, аналітики великих даних, блокчейн-технологій, квантових обчислень та Інтернету речей відкриває принципово нові можливості для прогнозування загроз, координації міжвідомчих дій, захисту критичної інфраструктури, протидії дезінформації. Однак технологічні інновації самі по собі не гарантують ефективності – необхідна системна трансформація інституційних структур, процесів прийняття рішень, організаційної культури та компетенцій персоналу.

Актуальність дослідження визначається кількома факторами. По-перше, тривала російсько-українська війна створює унікальну емпіричну базу для аналізу ефективності цифрових інструментів у протидії гібридним загрозам. По-друге, стрімкий розвиток технологій штучного інтелекту генеративного типу (ChatGPT, Midjourney тощо) радикально посилює можливості створення та поширення дезінформації, що вимагає нових підходів до захисту інформаційного простору. По-третє, досвід пандемії COVID-19 продемонстрував критичну важливість цифрової стійкості для забезпечення безперервності функціонування державних інституцій в умовах кризи. По-четверте, євроатлантична інтеграція України передбачає гармонізацію національних систем безпеки із стандартами НАТО та ЄС, що неможливо без масштабної цифровізації.

Огляд літератури. Проблематика цифрової трансформації національної безпеки перебуває на перетині кількох дослідницьких напрямів: теорії гібридної війни, студій кібербезпеки, публічного управління в умовах кризи, технологічних досліджень штучного інтелекту та великих даних.

Концептуалізація гібридної війни як окремого феномену відбулася у працях західних дослідників на початку XXI століття. Cornish у фундаментальному виданні «The Oxford Handbook of Cyber Security» систематизує виклики, які цифрова епоха створює для національної безпеки, наголошуючи на розмиванні кордонів між миром та війною, державними та недержавними акторами, військовими та цивільними технологіями [7]. Автор підкреслює, що кіберпростір став новим доменом конфлікту, де традиційні концепції стримування та відплати потребують переосмислення.

Murray та Mansoor у праці «Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present» простежують історичну еволюцію гібридних форм ведення війни, демонструючи, що поєднання регулярних та іррегулярних методів є константою військової історії, однак цифрові технології надають цьому явищу якісно нові характеристики [17]. Fox аналізує російську стратегічну традицію гібридної війни у тривіковому контексті, виявляючи взаємозв'язок між інформаційними операціями, дипломатичним тиском, економічною залежністю та воєнною загрозою [10].

Arutunyan у дослідженні «Hybrid Warriors» розкриває механізми, через які Росія використовує недержавних акторів – найманців, бізнесменів, політтехнологів – для реалізації своїх геополітичних цілей в Україні, демонструючи складність атрибуції відповідальності за гібридні атаки [2]. Brands у колективній монографії «War in Ukraine» аналізує наслідки російського вторгнення для глобального порядку, переосмислення стратегічних концепцій та трансформації військової справи [3].

Кібербезпека як критичний компонент національної безпеки досліджується у працях Kello «Striking Back: The End of Peace in Cyberspace», де автор критикує концепцію «кібер-легалізму» та пропонує стратегію «пунктирного стримування» (punctuated deterrence) – концентрованих відповідей на кумулятивний ефект кібератак замість реагування на кожен окремий інцидент [13]. Shackelford досліджує міжнародно-правові аспекти управління кіберзагрозами, пропонуючи модель поліцентричного регулювання [23]. Springer надає комплексний огляд сучасних форм кібервійни, включаючи російські атаки на українську інфраструктуру як кейс-стаді [24]. Brantly аналізує безпеку в кіберепосі через призму вразливостей цифрових систем та можливостей їх захисту [4].

Роль штучного інтелекту у національній безпеці розглядається у праці Kissinger, Schmidt та Huttenlocher «The Age of AI: And Our Human Future», де автори – державний діяч, технологічний лідер та академік – аналізують вплив ШІ на військову стратегію, розвідку, стримування та міжнародну стабільність [14]. Zegart у книзі «Spies, Lies, and Algorithms» досліджує трансформацію американської розвідувальної спільноти під впливом цифрових технологій, наголошуючи на необхідності переосмислення методів збору та аналізу інформації в епоху великих даних [27]. Casola та Papagianneas систематизують загрози та можливості, які ШІ створює для національної безпеки, включаючи автономні системи озброєнь, предиктивну аналітику та етичні дилеми [5].

Дезінформація як інструмент гібридної війни аналізується McIntyre у праці «On Disinformation», де розкривається історична спадкоємність між радянськими активними заходами та сучасними російськими кампаніями впливу [15]. Cosentino досліджує глобальну динаміку дезінформації у соціальних медіа в умовах пост-правди [8]. Rid у книзі «Active Measures» простежує еволюцію технік дезінформації від міжвоєнного періоду до сучасних інтернет-тролінгових ферм [22]. Woolley та Howard аналізують феномен обчислювальної пропаганди – використання ботів, алгоритмів та автоматизації для маніпулювання громадською думкою [26].

Цифрове врядування та його застосування у безпековому секторі розглядається у працях Milakovich «Digital Governance», де автор обґрунтовує необхідність переходу від електронного уряду до цифрового врядування як більш інтегрованої та орієнтованої на громадян моделі [16]. Giest та Roberge у міжнародному посібнику з цифрового врядування систематизують кращі практики впровадження цифрових технологій у публічному секторі різних країн, включаючи виклики штучного інтелекту [11]. Chen пропонує інтегровану рамку для управління цифровим врядуванням із фокусом на публічних цінностях [6].

Блокчейн-технології у контексті державного управління та безпеки досліджуються у колективних монографіях Pompella та Matousek щодо фінтеху та блокчейну [19], Reddick, Rodríguez-Bolívar та Scholl про блокчейн у публічному секторі [21], Tapscott та Tapscott щодо платформ та застосувань [25]. Ці праці розкривають потенціал розподілених реєстрів для забезпечення прозорості, незмінності записів та захисту критичних даних.

Український контекст гібридної війни аналізується у працях Plokhy «The Russo-Ukrainian War: The Return of History», де історик простежує глибинні корені конфлікту та його значення для глобального порядку [18]. D'Anieri досліджує динаміку українсько-російських відносин від розпаду СРСР до повномасштабної агресії [9]. Arel та Driscoll аналізують «неназвану війну» 2014-2022 років, розкриваючи механізми ескалації конфлікту [1]. Karatnycky та Ramani надають комплексний аналіз російської стратегії та української відповіді [12; 20].

Аналіз наукової літератури виявляє декілька прогалин. По-перше, бракує досліджень, які б інтегрували технологічний, інституційний, процесний та людський виміри цифрової трансформації національної безпеки у єдину концептуальну модель. По-друге, недостатньо проаналізовано специфіку застосування цифрових інструментів саме у контексті публічного управління (на відміну від військового застосування чи приватного сектору). По-третє, потребує систематизації досвід України як держави, яка протягом десятиліття протистоїть найбільш масштабній гібридній агресії в сучасній історії. Четверте, недостатньо розроблені практичні механізми імплементації цифрової трансформації з урахуванням обмежених ресурсів та спадщини застарілих систем.

Мета статті є розробка концептуальної моделі цифрової трансформації публічного управління національною безпекою в умовах гібридної війни та визначення пріоритетних напрямів і механізмів її реалізації на основі узагальнення міжнародного досвіду та особливостей українського контексту.

Методологія дослідження. Дослідження ґрунтується на комплексному застосуванні загальнонаукових та спеціальних методів пізнання. Системний

підхід використано для аналізу цифрової трансформації національної безпеки як цілісного феномену, що інтегрує інституційний, технологічний, процесний та людський виміри. Структурно-функціональний аналіз застосовано для виявлення взаємозв'язків між різними компонентами системи національної безпеки та визначення ролі цифрових технологій у їх функціонуванні. Компаративний метод використано для порівняльного аналізу досвіду різних країн у цифровізації безпекового сектору, виявлення кращих практик та можливостей їх адаптації в українських умовах. Метод теоретичного моделювання дозволив розробити концептуальну модель цифрової трансформації публічного управління національною безпекою з визначенням пріоритетних напрямів та механізмів реалізації. Кейс-метод застосовано для аналізу українського досвіду цифровізації в умовах активної фази війни, зокрема успішних ініціатив «Дія», кібервійськ, IT Army. Метод експертних оцінок використано для визначення критичності різних технологічних напрямів та інституційних механізмів. Емпіричну базу дослідження становлять офіційні документи міжнародних організацій (НАТО, ЄС), стратегічні документи провідних країн у сфері кібербезпеки та цифрової трансформації, статистичні дані щодо кіберінцидентів та дезінформаційних кампаній, а також наукові публікації у провідних міжнародних виданнях з питань національної безпеки, гібридної війни, кібербезпеки та цифрового врядування за період 2020-2024 років.

Основні результати дослідження. Цифрова трансформація публічного управління національною безпекою являє собою складний, багатовимірний процес, який виходить за межі простого впровадження нових технологій. Тому у даній статті ми пропонуємо концептуальну модель, яка інтегрує чотири взаємопов'язані виміри: інституційний, технологічний, процесний та людський.

Інституційний вимір охоплює створення нових організаційних структур, механізмів координації та моделей взаємодії між різними органами сектору безпеки. Традиційна фрагментація відповідальності між міністерствами оборони, службами безпеки, правоохоронними органами, кіберполіцією створює «сліпі зони» та уповільнює реагування. Цифровізація вимагає інституційної інтеграції через створення центрального координаційного органу, міжвідомчих робочих груп, спільних ситуаційних центрів. Критично важливою є розробка нормативно-правової бази, яка регулює обмін даними між відомствами при дотриманні принципів захисту персональної інформації та прав людини.

Технологічний вимір включає весь спектр цифрових інструментів, які можуть бути застосовані для посилення національної безпеки. Це не обмежується кібербезпекою, а охоплює штучний інтелект для аналізу загроз, великі дані для виявлення патернів, блокчейн для захисту критичних записів, квантові технології для захищеної комунікації, Інтернет речей для моніторингу інфраструктури, біометричні системи для ідентифікації. Ключовим є забезпечення інтероперабельності різних технологічних платформ та захисту від постійно еволюціонуючих кіберзагроз.

Процесний вимір стосується трансформації способів прийняття рішень, процедур реагування на інциденти, механізмів обміну інформацією. Гібридні загрози розгортаються зі швидкістю, яка вимагає практично миттєвого реагування – часові рамки для прийняття рішень скорочуються від днів до годин чи навіть хвилин. Це потребує делегування повноважень, автоматизації

рутинних процесів, створення чітких протоколів ескалації, впровадження систем підтримки прийняття рішень на основі ШІ. Водночас необхідні механізми людського контролю та перевірки для запобігання помилкам автоматизованих систем.

Людський вимір визнає, що технології самі по собі неефективні без людей, здатних їх належним чином використовувати. Це включає розвиток цифрових компетенцій персоналу безпекових структур, підготовку фахівців з кібербезпеки та даних-аналітиків, культурну трансформацію організацій від бюрократичної до інноваційної культури, залучення приватного сектору та громадянського суспільства. Особливу увагу необхідно приділити етичним аспектам використання ШІ, збереженню демократичного контролю та запобіганню зловживанням цифровими інструментами стеження.

Ці чотири виміри не є незалежними, а формують синергетичну систему. Технологічні інновації без інституційних реформ залишаться нереалізованими; інституційні зміни без відповідних компетенцій персоналу будуть неефективними; процесні оптимізації без технологічної підтримки не досягнуть необхідної швидкості. Тільки комплексна трансформація всіх чотирьох вимірів може забезпечити якісний стрибок у спроможностях системи національної безпеки протидіяти гібридним загрозам.

Причому одним з найбільш перспективних застосувань штучного інтелекту у національній безпеці є створення систем раннього попередження, здатних виявляти індикатори майбутніх загроз до їх матеріалізації. Машинне навчання може аналізувати величезні масиви даних з різнорідних джерел – відкритих публікацій, соціальних медіа, розвідувальних донесень, економічної статистики, супутникових знімків – для виявлення аномалій та прихованих патернів, які вказують на підготовку гібридних операцій.

Алгоритми обробки природної мови (NLP) здатні моніторити інформаційний простір у реальному часі, виявляючи скоординовані дезінформаційні кампанії на ранніх стадіях їх розгортання. Аналіз мережевої активності може ідентифікувати боти та тролінгові ферми, що поширюють маніпулятивний контент. Технології комп'ютерного зору дозволяють виявляти дипфейки – синтетичні відео та зображення, створені за допомогою генеративних нейромереж.

Предиктивна аналітика використовує історичні дані про минулі інциденти для прогнозування ймовірності майбутніх атак. Моделі можуть ідентифікувати вразливості критичної інфраструктури, прогнозувати цілі потенційних кібератак, оцінювати ризики дестабілізації у певних регіонах. Однак необхідно визнати обмеження таких систем – вони ефективні для виявлення відомих патернів, але можуть пропустити принципово нові форми загроз.

Проте критичним питанням залишається інтеграція різнорідних систем раннього попередження у єдину платформу, яка надає комплексну ситуаційну обізнаність особам, що приймають рішення. Необхідні інтерфейси візуалізації, які представляють складну інформацію у зрозумілій формі, механізми пріоритизації попереджень для уникнення інформаційного перевантаження, автоматизація передачі інформації відповідним органам для швидкого реагування.

Кібербезпека критичної інфраструктури – енергетичних систем, водопостачання, транспорту, фінансових мереж, систем охорони здоров'я,

урядових комунікацій – є наріжним каменем національної безпеки у цифрову епоху. Російські кібератаки на українську енергосистему у 2015-2016 роках продемонстрували спроможність супротивника створювати масштабні руйнування без фізичного проникнення на територію. У такий ситуації захист вимагає багаторівневого підходу: сегментація мереж для обмеження поширення атак, впровадження систем виявлення вторгнень (IDS) та запобігання вторгненням (IPS), безперервний моніторинг мережевого трафіку, регулярне оновлення програмного забезпечення та латання вразливостей, тестування на проникнення для виявлення слабких місць, резервне копіювання даних та плани відновлення після інцидентів. Особлива увага має приділятися захисту промислових систем управління (ICS/SCADA), які керують критичною інфраструктурою. Ці системи часто використовують застаріле програмне забезпечення, не призначене для роботи у ворожому кіберсередовищі, та мають обмежені можливості оновлення без зупинки виробничих процесів. Тому необхідні спеціалізовані рішення, які враховують специфіку промислових мереж, а блокчейн-технології можуть посилити кібербезпеку через незмінність записів, децентралізацію даних, криптографічний захист. Розподілені реєстри можуть використовуватися для захисту ланцюгів постачання, верифікації оновлень програмного забезпечення, забезпечення цілісності критичних даних. Квантові технології обіцяють якісно новий рівень захисту комунікацій, хоча їх широке впровадження ще попереду.

Наразі вже абсолютно зрозуміло, що дезінформація як інструмент гібридної війни становить особливий виклик для демократичних суспільств, які цінують свободу слова та уникають цензури. Російські інформаційні операції проти України та західних демократій демонструють складність маніпуляцій: створення псевдоньюсових сайтів, використання армій ботів та тролів, посилення поляризації через підтримку радикальних груп, створення альтернативних наративів історичних подій, підрив довіри до інституцій.

Цифрові технології можуть сприяти протидії дезінформації через декілька механізмів. Автоматизована верифікація фактів (fact-checking) використовує ШІ для порівняння тверджень з базами перевірених фактів та виявлення невідповідностей. Аналіз мережевої активності виявляє скоординовані кампанії ботів через патерни публікацій, час активності, мовні особливості. Технології виявлення дипфейків аналізують візуальні та аудіо артефакти, які видають синтетичний контент. У свою чергу, блокчейн може використовуватися для підтвердження автентичності контенту через криптографічне підписання оригінальних публікацій, створення незмінного запису про походження інформації, забезпечення можливості перевірки джерела. Це особливо важливо для медіа та урядових комунікацій. Однак технологічні рішення мають доповнюватися освітніми ініціативами з розвитку медіаграмотності населення, співпрацею з платформами соціальних медіа для швидкого видалення шкідливого контенту, підтримкою незалежної журналістики та фактчекінгу, стратегічними комунікаціями для проактивного формування наративів. Критично важливо уникати авторитарних підходів до регулювання інформаційного простору, які можуть нанести більшу шкоду демократії, ніж сама дезінформація.

Розвідувальна діяльність також зазнає радикальної трансформації під впливом цифровізації. Традиційна розвідка спиралася на людські джерела (HUMINT) та технічні засоби перехоплення (SIGINT), однак цифрова епоха

породжує нові форми: розвідка відкритих джерел (OSINT) через аналіз публічно доступної інформації в Інтернеті, кіберрозвідка (CYBINT) через моніторинг хакерських форумів та даркнету, соціальна медіа-розвідка (SOCMINT) через аналіз активності в соціальних мережах, геопросторова розвідка (GEOINT) через супутникові знімки та дані локації. Але великі дані (Big Data) трансформують аналітичні можливості розвідувальних служб. Алгоритми машинного навчання можуть обробляти петабайти інформації, виявляючи приховані зв'язки між особами, організаціями, фінансовими потоками, подіями, аналіз соціальних мереж розкриває структуру злочинних та терористичних організацій, фінансова розвідка простежує потоки незаконних коштів через блокчейн-транзакції.

Однак масштабне збирання даних породжує серйозні етичні та юридичні питання. Як збалансувати потреби національної безпеки та право на приватність? Як запобігти зловживанням інструментами масового стеження? Як забезпечити демократичний контроль та підзвітність розвідувальних служб? Ці питання особливо гострі в умовах, коли технології дозволяють не лише збирати дані про підозрілих осіб, але й вести тотальний моніторинг усього населення. Тому необхідні чіткі правові рамки, які визначають обмеження використання інструментів цифрової розвідки, процедури отримання санкцій для втручання у приватність, механізми нагляду з боку парламенту та судової влади, періодичний аудит дотримання процедур, захист викривачів незаконних практик. Демократичні суспільства повинні знайти баланс між безпекою та свободою, уникаючи як наївного лібертаріанства, так і авторитарного технологічного контролю.

Ефективність реагування на гібридні загрози критично залежить від швидкості та якості координації між різними органами. Традиційні канали міжвідомчої комунікації – офіційні листи, наради, телефонні дзвінки – занадто повільні та ненадійні в умовах кризи. Необхідні інтегровані цифрові платформи, які забезпечують захищений обмін інформацією у реальному часі, спільну ситуаційну обізнаність, координацію дій. Такі платформи мають включати: єдині бази даних про загрози та інциденти з контрольованим доступом для відповідних органів, системи обміну повідомленнями з наскрізним шифруванням, спільні електронні карти для візуалізації ситуації та координації операцій, інструменти відеоконференцій для проведення нарад без необхідності фізичної присутності, системи управління завданнями для відстеження виконання доручень, інтеграцію з аналітичними інструментами для підтримки прийняття рішень.

Криптографічний захист комунікацій є абсолютною необхідністю, оскільки супротивник здійснюватиме спроби перехоплення чутливої інформації. Квантово-стійка криптографія набуває особливого значення у світлі розвитку квантових комп'ютерів, які загрожують зламати існуючі криптографічні алгоритми. Багатофакторна автентифікація, біометрична ідентифікація, апаратні токени безпеки підвищують захист від несанкціонованого доступу.

Важливою є й інтероперабельність комунікаційних систем різних відомств та союзників. НАТО розробляє стандарти обміну інформацією між країнами-членами, які Україна має імплементувати в рамках євроатлантичної інтеграції. Спільні навчання та тренування відпрацьовують процедури взаємодії в умовах кризи, виявляють вузькі місця в координації, формують особисті зв'язки між представниками різних структур.

На наш погляд, успішна цифрова трансформація потребує центрального координаційного органу, який би забезпечував стратегічне планування, пріоритизацію ініціатив, мобілізацію ресурсів, контроль виконання. Цей орган може функціонувати при Раді національної безпеки і оборони України або безпосередньо підпорядковуватися Президенту чи Прем'єр-міністру.

Основні функції такого центру включають: розробку національної стратегії цифровізації безпекового сектору з визначенням пріоритетних напрямів, термінів, відповідальних виконавців та показників досягнення цілей; координацію діяльності різних міністерств та відомств для уникнення дублювання зусиль та забезпечення сумісності систем; акумуляцію та розподіл фінансових ресурсів через спеціальний бюджетний фонд цифрової трансформації безпеки; залучення експертизи з приватного сектору, академічних установ, міжнародних партнерів; моніторинг та оцінку ефективності впроваджених ініціатив через систему ключових показників; управління ризиками, пов'язаними з впровадженням нових технологій.

Відтак, центр має складатися з фахівців різних профілів: експертів з кібербезпеки, даних-аналітиків, фахівців з управління проектами, юристів, які спеціалізуються на приватності та захисті даних, представників користувачів – безпекових відомств. Саме такий мультидисциплінарний склад забезпечує комплексний підхід до проблем цифровізації. При цьому критичною є незалежність центру від окремих відомств, які можуть мати власні інституційні інтереси, що суперечать загальносистемній оптимізації. Підпорядкування центру безпосередньо вищому політичному керівництву надає йому необхідні повноваження для подолання міжвідомчих бар'єрів та забезпечення виконання рішень.

Поряд з цим інформаційна інтеграція є ключовою для ефективної протидії гібридним загрозам, оскільки індикатори атак часто розпорошені між різними відомствами. Спецслужби можуть володіти розвідувальною інформацією про підготовку операції, кіберполіція – даними про аномальну мережеву активність, прикордонна служба – інформацією про підозрілі переміщення, фінансова розвідка – сигналами про незвичайні транзакції. Тільки інтеграція цих фрагментів може дати цілісну картину загрози.

Міжвідомчі платформи обміну даними мають базуватися на принципах: федеративної архітектури, де кожне відомство зберігає контроль над своїми даними, але надає контрольований доступ іншим органам через стандартизовані інтерфейси; рольового доступу, який визначається потребою знати (need-to-know) та принципом мінімальних привілеїв; аудиту всіх звернень до даних для забезпечення підзвітності та виявлення зловживань; шифрування даних як при зберіганні, так і при передачі; стандартизації форматів даних та метаданих для забезпечення інтероперабельності. Технічною основою можуть бути системи класу «secure data-sharing platforms», які використовуються у провідних демократіях. Наприклад, у США Terrorism Information Awareness (TIA) об'єднує дані різних спецслужб при дотриманні строгих правил приватності. У Великобританії National Data Guardian встановлює стандарти обміну чутливими даними. Європейський Союз розробляє рамки для транскордонного обміну даними про безпеку між країнами-членами.

Юридичною основою має бути законодавство, яке чітко визначає: які категорії даних можуть бути поділені; за яких обставин та з якими обмеженнями; процедури отримання доступу до даних інших відомств;

відповідальність за неналежне використання інформації; права громадян на перевірку даних про них та виправлення помилок; механізми розгляду скарг на порушення.

Приватний сектор володіє передовими технологіями, талантами та інноваційною культурою, яких бракує урядовим структурам. Технологічні гіганти розробляють найсучасніші алгоритми ШІ, телекомунікаційні компанії управляють критичною інфраструктурою, кібербезпекові фірми мають експертизу у виявленні та нейтралізації загроз, стартапи пропонують інноваційні рішення. Тому ефективна цифровізація національної безпеки неможлива без тісної співпраці з бізнесом. При цьому форми державно-приватного партнерства можуть включати: спільні дослідницькі проекти з розробки нових технологій захисту критичної інфраструктури, систем виявлення загроз, протидії дезінформації; обмін інформацією про кіберзагрози, де бізнес надає дані про атаки на їхні системи, а уряд – розвідувальну інформацію про джерела загроз; аутсорсинг певних функцій кібербезпеки приватним компаніям з відповідною сертифікацією та безпековою перевіркою; спільні центри реагування на кіберінциденти (CERT/CSIRT), які координують дії між державним та приватним секторами; програми ротації кадрів між урядом та індустрією для обміну досвідом та створення міжсекторальних мереж; державні замовлення та гранти для стимулювання розробки необхідних технологій. Виклики при цьому включають: можливі конфлікти інтересів, коли компанії прагнуть максимізувати прибуток, а не захищати національну безпеку; ризики витоку чутливої інформації через залучення приватних підрядників; залежність від технологій окремих компаній, що створює вразливість; необхідність балансу між конфіденційністю безпекових операцій та комерційними інтересами бізнесу.

Гібридні загрози не визнають кордонів – кібератаки запускаються з територій інших держав, дезінформація поширюється через глобальні соціальні медіа, терористи використовують транснаціональні мережі фінансування. Це вимагає міжнародної кооперації у цифровізації національної безпеки. У цьому сенсі для України критичною є євроатлантична інтеграція – гармонізація систем національної безпеки зі стандартами НАТО та ЄС. НАТО розробила Cyber Defence Policy, яка визначає принципи колективної кіберзахисту, механізми обміну інформацією про загрози, спільні навчання та сертифікацію. Європейський Союз ухвалив NIS2 Directive (Network and Information Security), яка встановлює вимоги до кібербезпеки критичної інфраструктури, Digital Services Act для регулювання онлайн-платформ, AI Act для етичного використання штучного інтелекту. Інтеграція при цьому вимагає: імплементації міжнародних стандартів (ISO 27001 для управління інформаційною безпекою, NIST Cybersecurity Framework); участі у міжнародних механізмах обміну інформацією (NATO Cyber Defence Centre, EU Hybrid Fusion Cell); спільних навчаннях та тренуваннях (Cyber Coalition, Cyber Europe); взаємної юридичної допомоги у розслідуванні кіберзлочинів через Budapest Convention; технічної допомоги від партнерів для розбудови спроможностей.

Регіональна кооперація також важлива – співпраця з країнами Центральної та Східної Європи, які мають схожий досвід протистояння російським гібридним загрозам. Прибалтійські держави, Польща, Чехія

розробили ефективні моделі протидії дезінформації, зміцнення кіберзахисту, які можуть бути адаптовані в українських умовах.

Слід зазначити, що російсько-українська війна створила унікальну емпіричну базу для аналізу ефективності цифрових інструментів у протидії гібридним загрозам. Україна демонструє приклади успішної цифровізації навіть в умовах активних бойових дій. Так, застосунок «Дія» став символом цифрової держави, інтегруючи десятки державних послуг у єдиний інтерфейс смартфону. Під час війни функціональність розширилася на безпековий вимір: подання інформації про переміщення ворожої техніки через «єВорог», цифрові документи військовослужбовців, електронна взаємодія з тероборонми. Це демонструє, як цивільна цифрова інфраструктура може бути швидко адаптована для безпекових потреб.

IT Army of Ukraine – децентралізована мережа добровольців-хакерів, які здійснюють DDoS-атаки та інші кібероперації проти російських цілей. Це приклад «краудсорсингу» кібервійни, коли держава координує дії громадських активістів. Хоча юридичний статус таких формувань залишається дискусійним, їхня ефективність у перевантаженні ворожих систем очевидна.

Кібервійська України зазнали найбільш інтенсивних кібератак в історії – вайпери, що знищували дані, DDoS-атаки на урядові сайти, спроби вимкнення енергосистеми. Стійкість української цифрової інфраструктури, підтримана західними партнерами (Microsoft, Amazon, Google надали захищені хмарні сховища для критичних державних даних), стала несподіванкою для агресора. Це підкреслює важливість завчасної підготовки та резервування.

Протидія дезінформації здійснюється через StratCom (Центр стратегічних комунікацій), численні фактчекінгові організації (StopFake, VoxCheck), офіційні Telegram-канали, які оперативно спростовують фейки. Прозорість влади, швидкі брифінги, доступ журналістів до місць подій створюють «вакцину» проти ворожої пропаганди.

Супутниковий зв'язок Starlink від SpaceX забезпечив стійкі комунікації навіть після руйнування наземної інфраструктури, дозволивши збройним силам координувати дії, а цивільним – підтримувати зв'язок. Це демонструє критичну важливість резервних каналів комунікації.

Але попри безумовні успіхи, Україна стикається з серйозними викликами у цифровізації національної безпеки. По-перше, спадщина застарілих систем (legacy systems) – багато відомств досі використовують інформаційні системи, розроблені у 1990-2000-х роках, які несумісні з сучасними рішеннями. Модернізація вимагає значних інвестицій та часу.

По-друге, дефіцит кваліфікованих кадрів – фахівці з кібербезпеки, даних-аналітики, ШІ-інженери отримують значно вищі зарплати у приватному секторі та за кордоном. Держава не може конкурувати за таланти без реформування системи оплати праці у безпековому секторі. Військова мобілізація додатково скорочує доступний кадровий пул.

По-третє, обмежені бюджетні ресурси – війна поглинає левову частку державних видатків, залишаючи обмежене фінансування для цифровізації. Необхідна пріоритизація інвестицій у найкритичніші напрями та залучення міжнародної технічної та фінансової допомоги.

По-четверте, інституційна інерція – трансформація корпоративної культури бюрократичних організацій є повільним процесом. Опір змінам,

небажання ділитися інформацією між відомствами, прихильність до традиційних процедур гальмують впровадження інновацій.

По-п'яте, корупційні ризики – державні закупівлі цифрових систем можуть стати джерелом зловживань. Необхідні прозорі процедури тендерів, незалежний технічний аудит, громадський контроль.

По-шосте, вразливість до ворожого втручання – будь-які цифрові системи можуть стати ціллю кібератак. Впровадження нових технологій має супроводжуватися посиленням захисту. Залежність від іноземних технологічних платформ створює ризики політичного тиску.

Враховуючи зазначене та з урахуванням обмежених ресурсів та контексту війни, Україна має зосередитися на пріоритетних напрямах цифровізації національної безпеки:

Короткостроково (1-2 роки): зміцнення кіберзахисту критичної інфраструктури через впровадження сучасних систем виявлення вторгнень, резервування даних, тренування персоналу; розбудова спроможностей протидії дезінформації через автоматизоване виявлення координованих кампаній, підтримку фактчекінгу, медіаграмотність населення; інтеграція існуючих безпекових систем через міжвідомчі платформи обміну даними; залучення міжнародної технічної допомоги від НАТО та ЄС для навчання кадрів та передачі технологій.

Середньостроково (3-5 років): створення національної системи раннього виявлення загроз на основі ШІ, яка інтегрує дані з різних джерел; розгортання захищених комунікаційних платформ для міжвідомчої координації в умовах кризи; імплементація міжнародних стандартів кібербезпеки та інтероперабельності з союзниками; розбудова національних спроможностей з розробки критичних безпекових технологій для зменшення залежності від іноземних постачальників; формування резерву фахівців через програми державних стипендій, співпрацю з університетами, залучення діаспори.

Довгостроково (5-10 років): побудова цілісної цифрової екосистеми національної безпеки, де всі елементи – від локальних датчиків до стратегічних аналітичних центрів – інтегровані в єдину мережу; досягнення технологічного лідерства у окремих напрямах (наприклад, протидії дезінформації, де Україна має унікальний досвід); експорт українських безпекових технологій та експертизи іншим країнам, які протистоять гібридним загрозам; формування регіонального хабу кібербезпеки для Центральної та Східної Європи.

Причому критичним чинником успіху є політична воля керівництва, яке має зробити цифрову трансформацію безпеки національним пріоритетом, забезпечити необхідні ресурси, долати міжвідомчі бар'єри, залучати найкращі таланти незалежно від їхнього попереднього афіляції з державними структурами.

Висновки з даного дослідження і перспективи подальших досліджень. Цифрова трансформація публічного управління національною безпекою в умовах гібридної війни є не опційною модернізацією, а нагальною необхідністю виживання демократичних держав у XXI столітті. Гібридні загрози, які інтегрують кібератаки, дезінформацію, економічний тиск, дипломатичну війну та збройну агресію, створюють виклики, на які традиційні бюрократичні системи безпеки неспроможні ефективно відповісти.

Запропонована концептуальна модель інтегрує чотири критичні виміри трансформації: інституційний (нові структури координації та міжвідомчої

взаємодії), технологічний (штучний інтелект, великі дані, блокчейн, кібербезпека), процесний (швидкість та якість прийняття рішень), людський (компетенції та організаційна культура). Тільки синергія всіх чотирьох вимірів може забезпечити якісний стрибок у спроможностях системи національної безпеки.

Пріоритетними технологічними напрямами є: системи раннього виявлення загроз на основі машинного навчання, які аналізують величезні масиви даних для ідентифікації індикаторів майбутніх атак; кіберзахист критичної інфраструктури через багаторівневий підхід від сегментації мереж до квантової криптографії; протидія дезінформації через автоматизовану верифікацію фактів, виявлення ботів, блокчейн-автентифікацію контенту; цифрова розвідка, яка використовує відкриті джерела, соціальні медіа, аналітику великих даних; захищені комунікаційні платформи для координації дій різних відомств у реальному часі.

Інституційні механізми реалізації включають: створення центрального координаційного органу з повноваженнями стратегічного планування та контролю виконання; міжвідомчі платформи обміну даними з дотриманням принципів федеративної архітектури та рольового доступу; державно-приватне партнерство для залучення технологій та талантів бізнесу; міжнародну кооперацію та інтеграцію стандартів НАТО та ЄС.

Український досвід демонструє як можливості швидкої цифровізації навіть в екстремальних умовах активної фази війни (Дія, IT Army, кібервійська), так і структурні виклики (застарілі системи, дефіцит кадрів, обмежені ресурси, інституційна інерція). Стратегічні пріоритети для України включають короткострокову фокусацію на захисті критичної інфраструктури та протидії дезінформації, середньострокову розбудову інтегрованих систем виявлення загроз та координації, довгострокову побудову цілісної цифрової екосистеми та досягнення технологічного лідерства у окремих напрямах.

Критичним висновком є визнання, що ефективність цифрової трансформації залежить не лише від технологій, але від інституційних реформ, культурних змін, розвитку людського капіталу. Організації сектору безпеки мають трансформуватися від ієрархічних бюрократій до гнучких мережевих структур, від культури секретності до культури обміну інформацією (в рамках необхідних обмежень), від технофобії до активного експериментування з інноваціями.

Водночас необхідно зберігати баланс між безпекою та свободою, уникаючи створення авторитарних інструментів тотального контролю під приводом протидії загрозам. Демократичні суспільства мають розробити механізми використання цифрових технологій для посилення безпеки при збереженні права на приватність, свободи слова, демократичної підзвітності. Етичні принципи використання штучного інтелекту, захист персональних даних, судовий та парламентський нагляд за розвідувальними службами – все це не є перешкодами для ефективності, а навпаки, запобіжниками проти зловживань, які в довгостроковій перспективі можуть нанести більшу шкоду національній безпеці, ніж зовнішні загрози.

Перспективи подальших наукових розвідок включають: емпіричну оцінку ефективності різних цифрових інструментів протидії гібридним загрозам через порівняльний аналіз країн з різним рівнем цифровізації та інтенсивністю загроз; дослідження інституційних та культурних детермінант

успішності цифрової трансформації безпекових організацій; аналіз етичних дилем використання штучного інтелекту у національній безпеці та розробку нормативних рамок; вивчення потенціалу нових технологій (квантові обчислення, нейроінтерфейси, синтетична біологія) для безпеки та виклики, які вони створюють; дослідження моделей державно-приватного партнерства у сфері безпекових технологій в різних правових та культурних контекстах; порівняльний аналіз національних стратегій кібербезпеки та виявлення факторів ефективності; вивчення соціально-психологічних аспектів протидії дезінформації та розробку методів підвищення медіаграмотності населення. Практична значущість таких досліджень полягає у формуванні доказової бази для прийняття рішень щодо пріоритетів інвестицій у цифровізацію, ідентифікації найкращих практик, які можуть бути адаптовані в українських умовах, розробці конкретних рекомендацій для удосконалення державної політики у сфері національної безпеки та оборони.

Стаття надійшла до редакції 30.09.2025 р.
Стаття рекомендована до друку 08.11.2025 р.
Опубліковано 30.12.2025 р.

Dziundziuk Vyacheslav Borisovich,
Doctor of Science in Public Administration, Professor,
Head of Public Policy Chair,
Education and Research Institute of Public Administration, V. N. Karazin Kharkiv National University,
4, Svobody Sq., Kharkiv, 61022, Ukraine

e-mail: vbdzun@gmail.com *https://orcid.org/0000-0003-0622-2600*

DIGITAL TRANSFORMATION OF PUBLIC ADMINISTRATION OF NATIONAL SECURITY IN CONDITIONS OF HYBRID WARFARE

Abstract. The article examines the digital transformation of public administration systems for national security in the context of hybrid warfare. Based on an analysis of contemporary theoretical approaches and practical experience of leading countries, the features of digital technology application in countering hybrid threats are revealed. The necessity of transitioning from traditional bureaucratic security models to integrated digital ecosystems capable of promptly detecting, analyzing, and neutralizing multidimensional threats in real time is substantiated. A conceptual model of digitalization of the national security system has been developed, encompassing four key dimensions: institutional (creation of coordination structures and inter-agency cooperation mechanisms), technological (implementation of artificial intelligence, big data, blockchain, and cybersecurity), process-oriented (optimization of decision-making speed and response quality), and human (development of personnel digital competencies). Priority directions for digitalization have been identified: machine learning-based early threat detection systems, critical infrastructure cyber protection, disinformation countermeasures through automated content verification, digital intelligence and analytics, secure communication platforms for coordination. Special attention is given to institutional mechanisms for implementing digital transformation: establishing a coordination center, inter-agency data exchange platforms, public-private partnerships, and international cooperation. Using Ukraine as an example, challenges and opportunities for security sector digitalization during active warfare are analyzed, particularly successful digital initiatives such as «Diia,» cyber troops, and IT Army. It is established that the effectiveness of digital transformation depends on the synergy of technological innovations, institutional reforms, and cultural changes in security sector organizations. The proposed recommendations can be used to improve state policy in national security and defense.

Keywords: digital transformation, national security, hybrid warfare, public administration, cybersecurity, artificial intelligence, disinformation countermeasures, digital technologies.

REFERENCES

1. Arel, D., & Driscoll, J. (2023). Ukraine's Unnamed War: Before the Russian Invasion of 2022. Cambridge University Press.
2. Arutunyan, A. (2022). Hybrid Warriors: Proxies, Freelancers and Moscow's Struggle for Ukraine. Hurst Publishers.
3. Brands, H. (Ed.). (2024). War in Ukraine: Conflict, Strategy, and the Return of a Fractured World. Johns Hopkins University Press.
4. Brantly, A.F. (2023). Security in the Cyber Age. Cambridge University Press.
5. Casola, F., & Papagianneas, S. (Eds.). (2022). Artificial Intelligence and National Security. Springer.
6. Chen, Y.-C. (2015). Managing Digital Governance: Issues, Challenges, and Solutions. Routledge.
7. Cornish, P. (Ed.). (2021). The Oxford Handbook of Cyber Security. Oxford University Press.
8. Cosentino, G. (2020). Social Media and the Post-Truth World Order: The Global Dynamics of Disinformation. Palgrave Macmillan.
9. D'Anieri, P. (2023). Ukraine and Russia (2nd ed.). Cambridge University Press.
10. Fox, C.L. (2020). Hybrid Warfare. Georgetown University Press.
11. Giest, S., & Roberge, I. (Eds.). (2024). The Routledge International Handbook of Public Administration and Digital Governance. Routledge.
12. Karatnycky, A. (2024). Battleground Ukraine: From Independence to the War with Russia. Yale University Press.
13. Kello, L. (2022). Striking Back: The End of Peace in Cyberspace - And How to Restore It. Yale University Press.
14. Kissinger, H.A., Schmidt, E., & Huttenlocher, D. (2021). The Age of AI: And Our Human Future. Little, Brown and Company.
15. McIntyre, L. (2023). On Disinformation. MIT Press.
16. Milakovich, M.E. (2022). Digital Governance: Applying Advanced Technologies to Improve Public Service (2nd ed.). *Routledge.* https://doi.org/10.4324/9781003215875
17. Murray, W., & Mansoor, P.R. (Eds.). (2012). Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present. Cambridge University Press.
18. Plokhy, S. (2023). The Russo-Ukrainian War: The Return of History. W.W. Norton & Company.
19. Pompella, M., & Matousek, R. (Eds.). (2021). The Palgrave Handbook of FinTech and Blockchain. Palgrave Macmillan.
20. Ramani, S. (2023). Putin's War on Ukraine: Russia's Campaign for Global Counter-Revolution. Hurst Publishers.
21. Reddick, C.G., Rodríguez-Bolívar, M.P., & Scholl, H.J. (Eds.). (2021). Blockchain and the Public Sector: Theories, Reforms, and Case Studies. Springer.
22. Rid, T. (2020). Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux.
23. Shackelford, S.J. (2014). Managing Cyber Attacks in International Law, Business, and Relations. *Search of Cyber Peace*. Cambridge University Press.
24. Springer, P.J. (2022). Cyber Warfare. ABC-CLIO.
25. Tapscott, D., & Tapscott, A. (2023). Blockchains: A Handbook on Fundamentals, Platforms and Applications. Springer.
26. Woolley, S.C., & Howard, P.N. (2019). Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media. Oxford University Press.
27. Zegart, A.B. (2022). Spies, Lies, and Algorithms: The History and Future of American Intelligence. Princeton University Press.

The article was received by the editors 30.09.2025.
The article is recommended for printing 08.11.2025.
Published 30.12.2025.